

CALIFORNIA NOTICE AT COLLECTION AND PRIVACY POLICY FOR LIVING SPACES FURNITURE APPLICANTS

Rev. Date: January 1, 2023

Living Spaces Furniture, LLC (“**we**” or the “**Company**”) takes your privacy seriously. We want you to know how we collect, use, and disclose, your personal information.

This Privacy Policy explains:

1. The categories of personal information we collect about you;
2. The categories of sources from which we collect your personal information;
3. The purposes for which we use your personal information;
4. How we may disclose your personal information;
5. How long we keep your personal information;
6. Your privacy rights and how to exercise them; and
7. Changes to this Privacy Policy.

Scope:

This Privacy Policy applies to the personal information of individuals who are California residents in their role as job applicants to the Company (“**Applicants**”).

This Privacy Policy informs Applicants about the categories of personal information we have collected about them in the preceding twelve months as well as the categories of personal information that we will collect about Applicants in the future. This Privacy Policy does not apply to (a) employees of the Company (“**Team Members**”), (b) independent contractors, interns, volunteers, owners, board members, and other individuals who perform work for the Company (collectively “**Non-Employees**”), and (c) Team Members’ and Non-Employees’ dependents, emergency contacts, and beneficiaries (“**Related Contacts**”) (all collectively, “**Living Spaces HR Individuals**”) in their role as Living Spaces HR Individuals, or consumers.

“**Personal information**” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Applicant.

A subset of personal information is sensitive personal information which includes an individual’s social security number, driver’s license, state identification card, or passport number; account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; precise geolocation; racial or ethnic origin, religious beliefs, or union membership; content of communications (email, mail, or text), unless the business is the intended recipient; and genetic data. Sensitive personal information also includes processing of biometric information for the purpose of uniquely identifying personal information collected and analyzed concerning an individual’s health, sex life, or sexual orientation.

Personal information does not include:

- Publicly available information from government records.
- De-identified or aggregated information.
- Information excluded from the scope of the California Privacy Rights Act (“CPRA”), including:
 - health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data;
 - personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

1) INFORMATION THAT WE COLLECT

***These are examples under each category of personal information. Not all examples of personal information are actually collected.

Category	Examples Only
Identifiers	Legal name, preferred name, telephone number, postal address, e-mail address, signature, bank account name and number for direct deposits, and photographs
Professional or Employment-Related Information	Educational institutions attended, degrees and certifications, licenses, work experience and previous employers, professional memberships and affiliations, seniority, training, employment start and ending dates, and job title
Non-public educational information	Academic transcripts if provided
Commercial Information	Travel expense records for an interview
Internet Activity Information	Internet browsing and search history while using the Company’s network, log in/out and activity on the Company's electronic

	resources, interactions with the Company’s Internet web site, application, or advertisement, and publicly available social media activity
Sensory or Surveillance Data	Voicemails, recordings of meetings or video conferences, and footage from video surveillance cameras
Physical Description	Photograph if submitted as part of application materials
Preferences	Hobbies and leisure activities, membership in voluntary/charitable/public organizations, and preferences regarding work tools, travel, hours, and food for Company events
Characteristics of Protected Classifications Under state or Federal Law	Collected on a purely voluntary basis, except where collection is required by law, and used only in compliance with applicable laws and regulations, for diversity and inclusion reporting and related purposes; disability, medical condition, and pregnancy, childbirth, breastfeeding, and related medical conditions, as necessary to comply with Federal and state law related to accommodation
Sensitive identifiers	Social Security, driver's license, state identification card, or passport number
Geolocation data	IP Addresses
Health information	Information necessary to comply with Federal and state law related to accommodation
Personal communications	The contents of mail, email, or text messages on accounts or services not owned, or subscribed-to, by the Company to the extent required by law
Login credentials	Login credentials to an online account owned or subscribed-to by the Company
Religion	If volunteered in support of a request for a religious accommodation
Financial account access information	Payment card information with CVV and other information as needed for the HR Individual to purchase from the Company
Sexual orientation to the extent volunteered by the Applicant	For diversity and inclusion programs

2) THE SOURCES FROM WHICH WE COLLECT YOUR PERSONAL INFORMATION

- **You.** For example, in your job application, forms you fill out for us, surveys you complete, and any information you provide us during the course of your application and interview process.
- **Vendors and service providers.** For example, recruiters.
- **Third parties.** For example, job references, affiliated companies, professional employer organizations or staffing agencies.
- **Public internet sources.** For example, social media, job boards, public profiles, and other public online sources.

- **Public records.** For example, court records, and credentialing and licensing organizations.
- **Automated technologies** on Company's electronic resources. For example, to track logins and activity on the Company's careers page.
- **Surveillance/recording technologies installed by the Company.** For example, video surveillance in common areas of Company facilities, voicemail technologies, webcams, and audio/video recording technologies, any of these with consent to the extent required by law.
- **Government or administrative agencies.** For example, law enforcement or public health authorities.

Note: This Privacy Policy does not cover background screening conducted by third-party background check vendors subject to the federal Fair Credit Reporting Act. We provide separate notices/disclosures for such screening.

3) THE PURPOSES FOR WHICH WE USE YOUR PERSONAL INFORMATION

A. Generally Applicable Purposes

Unless stated otherwise in section 3.B, below, we may use Applicants' personal information for the following purposes:

Recruiting, including:

- To evaluate Applicants' qualifications or suitability for employment with the Company
- To communicate with Applicants
- To conduct a pre-employment or criminal history background check
- For identification purposes
- For diversity and inclusion purposes
- To arrange and manage Company-sponsored events
- To create a talent pool for future job openings
- For recordkeeping purposes
- To demonstrate Applicants' agreement to, or acceptance of, documents presented to them, *e.g.*, acknowledgment of employment application, offer letter
- To evaluate and improve the recruiting process
- To promote the Company as a place to work

Monitoring, Security, and Compliance, including:

- To monitor use of Company information systems and other electronic resources or information systems
- To conduct internal audits
- To conduct internal investigations

- To protect the safety and security of the Company's facilities
- To report suspected criminal conduct to law enforcement and cooperate in investigations
- To control access to secure facilities
- To monitor compliance with the Company's policies
- To exercise the Company's rights under applicable law and to support any claim, defense, or declaration in a case or before a jurisdictional and/or administrative authority, arbitration, or mediation panel

Conducting Our Business, including:

- For training purposes or quality assurance with respect to Company Team Members conducting the interviews or otherwise assisting with the recruiting and hiring process
- For travel and event planning
- To manage travel reimbursements

Miscellaneous Other Purposes:

- To manage and operate information technology and communications systems, risk management and insurance functions, budgeting, financial management and reporting, strategic planning;
- To manage litigation involving the Company, and other legal disputes and inquiries and to meet legal and regulatory requirements;
- In connection with a corporate transaction, sale, or assignment of assets, merger, divestiture, or other changes of control or financial status of the Company or any of its subsidiaries or affiliates; and
- To protect the rights, property, or safety of the Company, Living Spaces Team Members and other HR Individuals, guests/ customers, or others.

B. Purposes Specific To Certain Categories Of Personal Information

We may use the categories of Applicants' personal information listed in this Section 3.B for the purposes stated below:

Purposes For Using Applicants' Geolocation Data:

- Upon entry to the Company's facilities, the Company may issue Applicants an RFID-enabled security badge. The Company will use this information to protect the safety and security of its facilities and the people in its facilities, including the Applicant. The Company may also collect IP addresses when Applicants electronically sign documents submitted as part of their application process.

Purposes For Using Applicants' Health Information:

- To the extent necessary to comply with the Company's legal obligations, such as to accommodate disabilities
- To protect the health and safety of the Company's employees and facilities, for example, to take the Applicant's temperature
- For occupational health and safety compliance and record-keeping
- To conduct pre-employment medical examinations
- To respond to an Applicant's medical emergency

Note: This Privacy Policy does not cover health information governed by the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act), or California's Confidentiality of Medical Information Act (CMIA) because these laws have their own disclosure requirements.

Purposes For Using Applicants' Protected Categories Of Information:

The Company collects information about race, age, national origin, disability, sex, veteran status, and other protected categories as necessary to comply with legal obligations, including the reporting requirements of the federal Equal Employment Opportunity Act, and state laws, and for purposes of diversity analytics.

The Company also uses this personal information for purposes including: (a) with respect to disability and/or medical condition, as necessary, to comply with federal and state law related to accommodation; and (b) with respect to age, incidentally to the use of birth date for identity verification.

We collect personal information about membership in protected categories on a purely voluntary basis, except where required by law, and use the information only in compliance with applicable laws and regulations.

4) HOW WE MAY DISCLOSE YOUR PERSONAL INFORMATION

We generally maintain information related to Applicants as confidential. However, from time to time, we may have a legitimate business need to disclose Applicants' personal information for one of the purposes listed in Section 3, above, to one or more of the categories of external recipients listed below. In that event, we disclose your personal information and/or sensitive personal information only to the minimum extent necessary to achieve the purpose of the disclosure and only if the disclosure is permitted by the CPRA and other applicable laws.

- **Service providers and contractors:** we disclose your personal information to service providers and contractors for the purposes above to assist us in our recruiting efforts and in meeting our business needs and legal obligations.

- We share personal information with third party service providers and contractors who have entered into arrangements with us to access such personal information only for the purpose of performing services on our behalf and are expressly obligated not to disclose or use such personal information for any other purpose.
- Service providers and contractors include recruiters, law firms, travel agencies, and any other entity providing services to the Company.
- **Affiliated companies:** Other companies controlled by Living Spaces.
- **Government or administrative agencies:** These may include, for example:
 - Equal Employment Opportunity Commission, California Civil Rights Department, or other state equivalent as required to respond to employment claims and charges, and for reporting.
 - Law enforcement in the event of criminal investigations.
- **Required Disclosures:** We may be required to disclose personal information in a court proceeding, in response to a court order, subpoena, civil discovery request, other legal process, or as otherwise required by law.
- **Legal Compliance and Protections:** We may disclose personal information when we believe disclosure is necessary to comply with the law or to protect the rights, property, or safety of the Company, our guests/ customers, or others.

Disclosure for cross-context behavioral advertising:

Under the CPRA, California residents have the right to opt-out of sharing of personal information with third parties for cross-context behavioral advertising, provided that such third parties are not service providers or contractors. To the extent that we share such personal information for such purpose, we share that information with third party service providers and contractors who have entered into arrangements with us to access such personal information only for the purpose of performing services on our behalf and are expressly obligated not to disclose or use such personal information for any other purpose.

5) HOW LONG WE KEEP YOUR PERSONAL INFORMATION

If the Company hires you, the information collected about you during the job application process may become part of your personnel file and may be used to administer the employment relationship and for related reporting and recordkeeping purposes.

We retain your personal information as necessary to fulfill the purpose for which that information was collected and in accordance with applicable laws, including, but not limited to, the California Labor Code. If your personal information is no longer required, we will delete it or make it anonymous by removing all details that identify you. However, if necessary, we may retain your personal information for our compliance with any legal, accounting, or reporting obligation.

6) HOW TO EXERCISE CALIFORNIA PRIVACY RIGHTS FOR APPLICANTS WHO ARE CALIFORNIA RESIDENTS

Subject to applicable law, Applicants who reside in California have the following rights:

- **Right to Know:** You have the right to submit a verifiable request for copies of specific pieces of your personal information collected in the preceding 12 months and for information about the Company's collection, use, and disclosure of your personal information during that same 12-month time period.

Please note that the CPRA's right to obtain copies does not grant a right to the whole of any document that contains personal information, but only to copies of "specific pieces" of personal information. Moreover, Applicants have a right to know categories of sources of personal information and categories of external recipients to which personal information is disclosed, but not the individual sources or recipients. We do not always track individualized sources or recipients.

- **Right to Delete:** You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable request, we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

You should be aware that making a deletion request does not ensure complete or comprehensive removal or deletion of personal information or content you may have posted. In addition, if you continue as an Applicant, we will continue to collect information you share with us or we otherwise collect in connection with those interactions.

Under the California Privacy Rights Act, we may deny your deletion request if retaining the information is necessary for us or our service providers to:

1. Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing relationship with you, or otherwise perform a contract with you.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Debug products to identify and repair errors that impair existing intended functionality.
4. Exercise free speech, ensure the right of another to exercise their free speech rights, or exercise another right provided for by law.
5. Comply with the California Electronic Communications Privacy Act.

6. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.
 7. Enable solely internal uses that are reasonably aligned with expectations based on your relationship with us.
 8. Comply with a legal obligation.
 9. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.
- **Right to Correct:** You have the right to submit a verifiable request for the correction of inaccurate personal information maintained by the Company that is objectively false information, taking into account the nature of the personal information and the purposes of processing the personal information.
 - **Right to Restrict Use and Disclosure of Sensitive Personal Information:** You have the right to restrict the Company's use and disclosure of your sensitive personal information to purposes permitted under the CPRA, such as security, quality control, uses required by law, and disclosures to vendors in support of the permitted purposes. This right only applies to sensitive personal information collected or processed by Company for the purpose inferring characteristics about you. The Company does not collect or process your sensitive personal information for the purpose inferring characteristics.

Note on Deidentified Information

At times, we convert personal information into deidentified information using reasonable measures to ensure that the deidentified information cannot be associated with the individual ("Deidentified Information"). We maintain Deidentified Information in a deidentified form and does not attempt to reidentify it, except that we may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes ensure that the information cannot be associated with the individual. We prohibit vendors, by contract, from attempting to reidentify the Company's Deidentified Information.

a. How to Exercise Your Rights

To exercise the access, correction and deletion rights described above, please submit a verifiable request to us by either:

- Calling us at 714-735-3618.
- Visiting www.livingspaces.com/HRprivacyrequest

Only you or an authorized agent registered with the California Secretary of State that you have authorized to act on your behalf may make a verifiable request. If a request is made through an agent, we may require proof that the agent has been authorized by you.

You may only make a verifiable request for access twice within a 12-month period. The verifiable request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity to make the request and confirm the personal information relates to you (or an agent is unable to provide proof that the agent has been authorized by you).

In connection with verifying your identity, we will request that you provide certain data points (e.g., name, email address, phone number, address, etc.) so that we may match those with data points maintained by us (so that we may verify your identity with a reasonable degree, or in some cases depending on your request, with a reasonably high degree, of certainty). This will require us being able to match at least two data points and in many cases, including those requests for specific pieces of personal information, at least three data points provided by you with personal information maintained by us. Any request for specific pieces of information will also require that you declare under penalty of perjury that the request relates to you.

Response Timing

We shall attempt to respond to a verifiable request within 45 days of its receipt. If we require more time (up to 90 days), we will inform you of the extension period in accordance with the California Privacy Rights Act.

c. The Company's Non-Discrimination and Non-Retaliation Policy

We will not unlawfully discriminate or retaliate against you for exercising your privacy rights under the California Privacy Rights Act or as otherwise set forth in other state equivalent.

7) CHANGES TO THIS PRIVACY POLICY

If we change this Privacy Policy, we will post those changes on this page and update the Privacy Policy modification date above. If we materially change this Privacy Policy in a way that affects how we use or disclose your personal information, we will provide a prominent notice of such changes and the effective date of the changes before making them.

For More Information

For questions or concerns about the Company's privacy policies and practices, please visit www.livingspaces.com/HRprivacyrequest.